

English translation of the amended sheets of
International Preliminary Examination Report

CLAIMS

1. Processing procedure for an electronic system
subject to transient error constraints, characterised
5 in that in a given real time cycle, in other words in a
give operational cycle of a software task that is
executed periodically and continuously, two virtual
sequences located on a single physical sequence are
multiplexed in time (the data resulting from each
10 execution of a virtual sequence being stored so that
they can be voted before use), and in that if an error
is detected, the real time cycle in progress is
inhibited and a healthy context is reloaded to make a
restart that consists of a nominal execution of the
15 next cycle starting from the reloaded context

2. Process according to claim 1, in which three
error confinement areas (time, software and hardware)
are used.

20

3. Process according to claim 1, in which a memory
plane in the control unit is used, protected from
singular events by an error detection and correction
code.

25

4. Process according to claim 1, in which the
detection / correction granularity used is the computer
operational cycle.

ART 34 AMDT

English translation of the amended sheets of
International Preliminary Examination Report

5. Process according to claim 1, in which the
"backup context" function activated regularly is
achieved by means of an index change.

5 6. Process according to claim 1, in which the
"restore context" function activated during an error
correction is performed due to the fact that the index
indicating the context considered to be healthy, in
other words error free, after the previous operational
10 cycle has not changed, even though it has usually
swapped, in other words no errors are detected; this
"no swap" being inherent to inhibition of the real time
cycle in which the error is detected.

15 7. Process according to claim 1, in which
segmentation of the memory is associated with a
hardware device to check access rights.

20 8. Process according to claim 7, in which the
hardware device to check access rights enables several
access configurations, each configuration allowing
access to one or several non-contiguous segments.

25 9. Process according to claim 7, in which the
hardware device to check access rights is used to
select several access configurations with logical
combinations of one or several keys.

ART 34 AMDT

English translation of the amended sheets of
International Preliminary Examination Report

10. Process according to claim 1, in which the
variables / data to be voted are put into a table.

11. Process according to claim 1, in which a
5 software vote is used for which integrity is achieved
by software checks, particularly including a software
and hardware monitoring processor.

10 12. Process according to claim 1, in which a
transfer to the control electronics is controlled by a
hardware device that checks access rights and limits
the validity of this transfer in time, thus delimiting
an hardware error confinement area.

15 13. Process according to any one of the previous
claims, used in space applications.

20 14. Device for monitoring memory accesses in a
computer comprising a control unit built around a
microprocessor and a memory, characterized in that the
memory is partitioned into segments, in that each
segment has an access right defined by a logical
function of all or some of the keys available in the
25 device, the access right to each segment being checked
in real time, and in that access for some segments will
only be authorized if there is a very strong
probability that the microprocessor will be in a good

English translation of the amended sheets of International Preliminary Examination Report operating state, thus enabling safe storage of critical data.

15. Device according to claim 14, in which a set
5 of non-contiguous segments is accessible, in read only for some segments and in read / write for other segments, depending on the programming of the keys present in the device.

10 16. Device according to claim 14 in which the segment size is arbitrary, so that it can be optimised for a given application.

15 17. Device according to claim 14, in which definitions of the set of available keys, the logical combination functions for these keys and the configuration of the accessible segments as a function of the programming of the keys, are specific.

20 18. Device according to claim 14, in which one of the segments has a write authorization accessible in an exceptional state of the computer, thus enabling safe storage of critical data. *a*

25 19. Device according to claim 14, in which segments enabling safe storage of critical data are stored by pair, working in flip-flop.

ADD a21